明 細 書

量子暗号通信装置

技術分野

この発明は、位相変調方式の量子暗号において、送信者側で量子を秘密情報で変調した後伝送し、受信者側で受信した量子を復調することで秘密情報を共有する量子暗号通信装置に関するものである。

背景技術

量子暗号通信とは、送信者側が量子、一般的には光子を秘密情報で変調した後伝送し、受信者側が受信した量子を復調することで秘密情報を共有する通信方式である。量子に載せられた秘密情報は量子力学の不確定性原理により安全性が保証されている。但し、量子は壊れやすく、全ての情報を確実に伝送できるわけではないため、秘密情報としては乱数情報を用いている。送受信者間で伝送される乱数情報は、誤り訂正や守秘性を高める等のデータ処理を行った後、暗号通信用の秘密鍵として用いられる。これを特に量子鍵配布と呼んでいる。

ところで、位相変調方式は、光ファイバ通信をベースにした量子暗号において好適に用いられる変調方式である。これは、信号光パルスと参照光パルスという時間差２連光子パルスの相対位相情報が光ファイバ伝送中に比較的よく保存されるためである。相対位相情報は、信号光パルスと参照光パルスとを合波した際に生じる干渉現象を観測することで復調できる。このため、位相変調方式の量子暗号通信装置では、送信装置側に２連光子パルスを発生させるための非対称マッハツェンダ干渉計と呼ばれるループ状光路を持ち、受信装置側に２連光子パルスを合波、干渉させるための同じ大きさの非対称マッハツェンダ干渉計を持つ構成が一般的である。

しかしながら、このような構成の量子暗号通信装置においては、以下の２つの揺らぎの効果が無視できない影響を及ぼしている。１つは、通信路の持つ複屈折性の偏波揺らぎであり、もう１つは、送受信装置が持つ２つの非対称マッハツェ

ンダ干渉計の間に生じる光路長揺らぎである。この２つの揺らぎのため、上記構成の量子暗号通信装置では絶え間ない偏波および光路長の調整が必要であった。

これに対して、デファクト化が進行している。プラグ＆プレイ方式と呼ばれる量子暗号通信装置は、量子受信装置から量子送信装置へ、量子送信装置から量子受信装置へと２連光子パルスを往復させ、量子送信装置内で非相反的に各光パルスの偏波面を直角に回転させた後反射することで、量子伝送路上で被る偏波揺らぎを往路と復路とで相殺し、偏波揺らぎの自動補償を実現している。また、量子受信装置内で信号光と参照光という時間差のある２連光子パルスを発生させるためのループ状光路と２連光子パルスを合波、干渉させるためのループ状光路とを同一にすることで、光路長揺らぎの補償された安定な合波、干渉を実現していた（例えば、特許文献１及び３、非特許文献１参照）。

なお、上記のようなプラグ＆プレイ方式の量子暗号通信装置において、特に量子送信装置を構成する光学系の１構成例として、量子暗号に特化した光学系ではないが、偏波回転ミラーを用いた光学系の構成も可能である（例えば、特許文献２参照）。

特許文献１：特開２００２－２８９２９８号公報（段落００３３、図１）

特許文献２：特開平５－２４１１０４号公報（段落００１２、図４（ａ）、図５（ｂ））

特許文献３：ＵＳ６，１８８，７６８Ｂ１（図２，図４及び第６頁）

非特許文献１：G. Ribordy, et. al. "Automated "Plug & Play" Quantum Key Distribution" Electronics Letters 34, (22), pp. 2116-2117, 1998

従来のプラグ＆プレイ方式の量子暗号通信装置は、光子パルスが同一光路上を往復することで揺らぎに対して安定な系を構成しているが、このために、光子パルスが量子受信装置内の位相変調器を往路と復路とで２回通過しなければならない。通信速度を高速にするために光源の繰り返し周波数を上げていき、光子パルスが光路を往復するのにかかる時間よりも短い周期で光子パルスが発振されるようになると、１周期の中での往路光子パルスが位相変調器を通過するタイミングと復路光子パルスが位相変調器を通過するタイミングが接近し、選択した繰り返し周波数によっては復路光子パルスのみに位相変調をかけるつもりでも、位相変

調不要な往路光子パルスにも位相変調がかかってしまうという問題点があった。

この発明は上記のような問題点を解決するためになされたもので、往路光子パルスに位相変調がかかることを防ぎ、通信速度高速化のために光源の繰り返し周波数を自由に選択できる量子暗号通信装置を得ることを目的とする。

発明の開示

この発明に係る量子暗号通信装置は、量子を伝送するための量子通信路と、前記量子伝送路の送信側に設置された量子送信装置と、前記量子伝送路の受信側に設置された量子受信装置と、前記量子送信装置と前記量子受信装置を結合して同期信号を含む制御信号を相互通信するための制御信号通信路とを備えた量子暗号通信装置であって、前記量子受信装置は、量子源となる光源と、前記光源から出た光子パルスから信号光パルスと参照光パルスとの時間差２連光子パルスを発生すると共に、逆進する量子である信号光パルスと参照光パルスとを合波、干渉させるための合波干渉手段を有するループ状光路と、前記量子通信路との接続口に設けられて、前記時間差２連光子パルスが前記量子通信路を介して前記量子送信装置と前記量子受信装置との間を往復した後、受信される前記参照光パルスのみに対して位相変調をかける位相変調器を有する迂回光路と、前記ループ状光路を介した干渉光を観測する光子検出器とを含み、前記量子送信装置は、前記量子受信装置から前記量子通信路を介して到達した２連光子パルスの偏波面を非相反的に直角に回転させる偏波回転手段と、前記偏波回転手段を通過した信号光パルスに位相変調をかけて再び量子通信路を通って前記量子受信装置に戻す位相変調器と、信号光パルスをパルス中に光子が２個以上含まない状態まで減光する減光手段とを含むことを特徴とする。

図面の簡単な説明

図１は、この発明の実施の形態１に係る量子暗号通信装置を示す構成図、

図２Ａは、図１に示す非対称マッハツェンダ干渉計と位相変調器用迂回光路の構成図、

図２Ｂは、図２Ａの位相変調器用迂回光路の変形構成図、

図２Ｃは、図２Ａの非対称マッハツェンダ干渉計の変形構成図、

図２Ｄは、図２Ａの非対称マッハツェンダ干渉計の変形構成図、

図３Ａは、図１に示す量子送信装置の光学系の構成図、

図３Ｂは、図１に示す量子送信装置の光学系の変形構成図、

図３Ｃは、図１に示す量子送信装置の光学系の変形構成図、

図３Ｄは、図１に示す量子送信装置の光学系の変形構成図、

図３Ｅは、図１に示す量子送信装置の光学系の変形構成図、

図４は、図１に示すこの発明の実施の形態１による量子通信動作を説明するフローチャート、

図５は、この発明の実施の形態２に係る量子暗号通信装置を示す構成図、

図６Ａは、図５に示す量子受信装置の光学系の構成図、

図６Ｂは、図５に示す量子受信装置の光学系の変形構成図、

図６Ｃは、図５に示す量子受信装置の光学系の変形構成図、

図６Ｄは、図５に示す量子受信装置の光学系の変形構成図、

図６Ｅは、図５に示す量子受信装置の光学系の変形構成図、

図７は、図５に示すこの発明の実施の形態２による量子通信動作を説明するフローチャートである。

発明を実施するための最良の形態

実施の形態１.

図１は、この発明の実施の形態１に係る量子暗号通信装置を示す構成図であり、光ファイバに基づく位相変調方式を用いた装置の全体構成を示している。

図１に示す量子暗号通信装置は、送信側の量子送信装置１００と、受信側の量子受信装置２００と、量子送信装置１００および量子受信装置２００を相互接続するための量子伝送路となる光ファイバ通信路１と、公開通信路２および制御信号通信路３とにより構成されている。

量子送信装置１００および量子受信装置２００は、量子として振舞う光子を伝送する光ファイバ通信路１と、ＬＡＮやインターネットで代表される公開通信路２と、制御信号通信路３とを介して相互に接続される。

光ファイバ通信路１は、量子暗号を含む量子信号を伝送し、制御信号通信路３は、量子送信装置１００および量子受信装置２００を同期・調歩動作させるための制御信号を伝送する。また、制御信号通信路３としては、具体的には、光ファイバ通信路１または公開通信路２が用いられてもよい。

量子送信装置１００は、前述した特許文献２に記載された光学系と類似の構成を有しており、光ファイバ通信路１に一端が接続されたアッテネータ１４と、アッテネータ１４の他端の光路に接続された偏光ビームスプリッタ１５と、偏光ビームスプリッタ１５の２つの光路に個別に接続されたファラディー回転子１６および位相変調器１７と、位相変調器１７を制御する送信側制御手段２０と、送信側制御手段２０に接続されて第１の乱数を出力する送信側データ処理手段２２とを備えている。

偏光ビームスプリッタ１５、ファラディー回転子１６および位相変調器１７は、量子通信用の光子パルスに対する両回転方向の光路ループを構成しており、量子送信装置１００は、量子受信装置２００から導入された光子パルスを、光ファイバ通信路１およびアッテネータ１４を介してファラディー回転子１６に導入し、非相反的に偏波面を直角に回転させる偏波回転手段としてのファラディー回転子（非相反素子）１６を通した後、再度アッテネータ１４および光ファイバ通信路１を介して量子受信装置２００に向けて反射して戻すようになっている。なお、アッテネータ１４は、信号光パルスをパルス中に光子が２個以上含まない状態まで減光する減光手段をなす。

一方、量子受信装置２００は、量子源となる光子を発生する光源としての光子発生器４と、光子発生器４の出力光路に一端が接続された偏光子５と、偏光子５の他端にＰ偏光出力ポートが接続された偏光ビームスプリッタ６と、偏光ビームスプリッタ６のＳ偏光出力ポートに接続された光子検出器１９と、偏光ビームスプリッタ６の合波光入力ポートに配設されたビームスプリッタ７、８およびミラー９、１０からなる非対称マッハツェンダ干渉計と、非対称マッハツェンダ干渉計のビームスプリッタ７の残った出力ポートに接続された光子検出器１８と、非対称マッハツェンダ干渉計のビームスプリッタ８の出力ポートに合波光入力ポートが接続された偏光ビームスプリッタ１１と、偏光ビームスプリッタ１１のＳ偏

光出力ポートに接続された位相変調器１３と、偏光ビームスプリッタ１１のＰ偏光出力ポートにＰ偏光出力ポートが接続され、かつ、位相変調器１３の他端がＳ偏光出力ポートに接続され、かつ、合波光入力ポートが光ファイバ通信路１に接続された偏光ビームスプリッタ１２と、光子検出器１８、１９の検出信号を取り込み、かつ、位相変調器１３と光子検出器１８、１９と光子発生器４を制御する受信側制御手段２１と、受信側制御手段２１に接続されて第２の乱数を出力し、光子検出信号を入力する受信側データ処理手段２３とを備えている。

量子受信装置２００内の偏光ビームスプリッタ１２は、光ファイバ通信路１を介して量子送信装置１００内のアッテネータ１４に接続され、受信側制御手段２１は、制御信号通信路３を介して送信側制御手段２０に接続され、受信側データ処理手段２３は、公開通信路２を介して送信側データ処理手段２２に接続されている。

量子受信装置２００内において、ビームスプリッタ７、８およびミラー９、１０からなる非対称マッハツェンダ干渉計は、光子発生器４から発生した光子パルスを信号光パルスと参照光パルスとの時間差２連光子パルスに分離するループ状光路を形成し、ここで、ビームスプリッタ７は、逆進する量子である信号光パルスと参照光パルスとの合波、干渉を引き起こす合波干渉手段として機能する。

また、量子受信装置２００内において、偏光ビームスプリッタ１１、１２は、２つの直交する偏波モードを分離し、Ｐ偏光した光子が量子受信装置２００から量子送信装置１００へ伝送する際には、偏光ビームスプリッタ１１、１２を短絡する光路が選択され、Ｓ偏光した光子が量子送信装置１００から量子受信装置２００へ伝送する際には、位相変調器１３を経由する迂回光路が選択される。

次に、図１に示したこの発明の実施の形態１に係る量子暗号通信装置の動作について説明する。

受信側制御手段２１は、制御信号通信路３を介した制御信号の相互通信により、量子送信装置１００内の送信側制御手段２０と同期・調歩動作する。

量子受信装置２００内の光子発生器４は、受信側制御手段２１が出力する同期信号に応じて偏波面の揃った光子パルスを発生する。

光子発生器４から発生した光子パルスは、偏光ビームスプリッタ６のＰ偏光に

あたる偏波面のみが通過するように設置されている偏光子５によって、偏波面が整えられた後、非対称マッハツェンダ干渉計に入光する。非対称マッハツェンダ干渉計に入光した光子パルスは、偏波面の揃った可干渉な時間差を有する参照光パルスと信号光パルスと呼ばれる２連光子パルスに分離され、偏光ビームスプリッタ１１に導かれる。

ここで、２連光子パルスのうち先行する第１の光子パルス（参照光パルス）は、ビームスプリッタ７から直にビームスプリッタ８へ進行した光子パルスであり、他方の後続する第２の光子パルス（信号光パルス）はビームスプリッタ７で反射されてミラー９、１０を通過する光子パルスである。偏光ビームスプリッタ１１に導かれた２連光子パルスは、偏光ビームスプリッタ６と同じに偏光面が設定されている偏光ビームスプリッタ１１、１２をこの順に通過し、位相変調器１３のある迂回光路に導かれることなく、光ファイバ通信路１に導かれる。

なお、図１における非対称マッハツェンダ干渉計と位相変調器用迂回光路の構成例としては種々採用できる。図２Ａは、図１に示す非対称マッハツェンダ干渉計の構成例であり、ビームスプリッタ７、８とミラー９、１０とを用い、位相変調器用迂回光路の構成例として、１×２（１入力２出力または２入力１出力）タイプの偏光ビームスプリッタ１１、１２とで２式を用いた構成例を示したが、図２Ｂに示すように、２×２（２入力２出力または２入力２出力）タイプの偏光ビームスプリッタ２４を１式用いた迂回光路の構成例や、図２Ｃに示すように、カプラ２５、２６と遅延ファイバ２７を用いた非対称マッハツェンダ干渉計の構成例や、図２Ｄに示すように、カプラ２８とファラディーミラー２９、３０を用いた非対称マッハツェンダ干渉計の構成例も存在し、特定の１つの構成例に特化されるものではない。なお、図２Ｄにおいて、３１はサーキュレータを示す。

量子受信装置２００から光ファイバ通信路１に導かれた２連光子パルスは、量子送信装置１００に導入され、量子送信装置１００内のファラディー回転子１６により偏波面を非相反的に直角に回転させられ、位相変調器１７により信号光パルスが位相変調を受けた後、再び量子受信装置２００に帰還してくる。

なお、図１における量子送信装置の光学系の構成例としては種々採用できる。図３Ａは、図１に示す量子送信装置の光学系の構成例であり、アッテネータ１４

と偏光ビームスプリッタ１５とファラディー回転子１６と位相変調器１７を用いた構成例を示したが、図３Ｂに示すように、２個の１×２偏光ビームスプリッタ３２，３３、２個の位相変調器３４，３５およびファラディーミラー３６を用いた構成例や、図３Ｃに示すように、２個の１×２偏光ビームスプリッタ３７，３８、位相変調器３９およびファラディーミラー４０を用いた構成例や、図３Ｄに示すように、２×２偏光ビームスプリッタ４１、位相変調器４２およびファラディーミラー４３を用いた構成例や、図３Ｅに示すように、偏波無依存の位相変調器４４およびファラディーミラー４５を用いた構成例も存在し、１つの構成例に特化されるものではない。

量子受信装置２００に帰還した２連光子パルスは、偏光ビームスプリッタ１２で完全に反射されて、位相変調器１３が配置された迂回光路に導かれる。なぜならば、光ファイバ通信路１の一方の端点で入射された光が他方の端点で非相反的に直角に偏波面の回転を受けて反射して帰還する場合に、途中の光路でいかなる複屈折性の揺らぎが存在したとしても、入射した時点から直角に偏波面が回転した状態で帰還するからである。

偏光ビームスプリッタ１２で反射された２連光子パルスは、位相変調器１３に入光する。このとき、位相変調器１３は、受信側制御手段２１の制御下で、受信側データ処理手段２３が出力した第２の乱数に応じて、参照光パルスのみに対して位相変調をかける。

位相変調器１３を通過した２連光子パルスは、偏光ビームスプリッタ１１で完全に反射されて非対称マッハツェンダ干渉計へと導かれる。このとき、非対称マッハツェンダ干渉計は、先行する参照光パルスを時間差の有する参照光２連光子パルス、すなわち、ビームスプリッタ８からビームスプリッタ７に直行する参照光の先行光子パルスと、ミラー１０、９を通過する参照光の後続光子パルスに分割し、同様に後続する信号光パルスを、時間差の有する信号光２連光子パルス、すなわち、ビームスプリッタ８からビームスプリッタ７に直行する信号光の先行光子パルスと、ミラー１０、９を通過する信号光の後続光子パルスに分割する。

ここで、非対称マッハツェンダ干渉計で往路、復路ともに同じ光路を用いているので、各２連光子パルスの各時間差は自動的に全く同じとなる。

従って、参照光の後続光子パルスと信号光の先行光子パルスは同時にビームスプリッタ７に到達して干渉を引き起こすことになる。干渉を引き起こした光子パルスは、排他的に１対の光子検出器１８、１９のいずれかに接続する一方のポートに導かれ、一方の光子検出器を発火する。なお、光子検出器１９に接続するポートに導かれた光子パルスは、偏光ビームスプリッタ６により完全に反射されて、光子検出器１９に導かれることになる。

受信側制御手段２１は、光子検出器１８、１９のいずれが発火したかをビット情報に変換し、受信側データ処理手段２３に伝送する。受信側データ処理手段２３は、第２の乱数と、量子情報で伝送されたビット情報とから、公開通信路２を用いて、量子送信装置１００と情報の一部を交換しつつ、秘匿性が保証されたランダムな情報を共有する。

次に、量子送信装置１００に注目しながら、具体的な動作について説明する。

量子受信装置２００から光ファイバ通信路１を通過して量子送信装置１００に導入された２連光子パルスは、量子送信装置１００に到達した時点では、光ファイバ通信路１の有する複屈折性の揺らぎにより偏波面が完全にランダムな状態になっている。この状態で、量子送信装置１００に導入された２連光子パルスは、アッテネータ１４で減衰された後、偏光ビームスプリッタ１５によりそれぞれ直交する２つの偏波モード（Ｐ偏光とＳ偏光）に分離される。

このようにして、４つに分離された光子パルスのうち、時計回りに進行する２連光子パルス（Ｓ偏光）は、偏光ビームスプリッタ１５で反射され、位相変調器１７を通過した後、ファラディー回転子１６で非相反的に偏波面を直角に回転させられた後、偏光ビームスプリッタ１５に戻る。

また、４つに分離された光子パルスのうち、反時計回りに進行する２連光子パルス（Ｐ偏光）は、偏光ビームスプリッタ１５を通過し、ファラディー回転子１６で非相反的に偏波面を直角に回転させられて、位相変調器１７を通過した後、偏光ビームスプリッタ１５に戻る。

このとき、位相変調器１７は、送信側制御手段２０の制御下で、送信側制御手段２２が出力した第１の乱数に応じて、２連光子パルスのうち信号光パルスのみに対して、時計回りまたは反時計回りの進行方向に依存することなく、位相変調

器１７を通過する際に位相変調をかけている。

偏光ビームスプリッタ１５に戻った４つの光子パルスは分離合流するまでの光路長が、時計回りまたは反時計回りに依存せずに等しいので、再び２連光子パルスとなり、アッテネータ１４に導入される。

ここで、アッテネータ１４の光子レベル強度の減衰の大きさは、信号光パルスの光子数が「１」を越えない強度となるように調整されている。

このようにして、再び光ファイバ通信路１に導入されて量子受信装置２００に帰還した２連光子パルスは、前述したとおり、偏光ビームスプリッタ１２により完全に反射されて、位相変調器１３のある迂回光路を通った後、偏光ビームスプリッタ１１で反射されて、光子検出器１８、１９の設置されたポートに導かれる。

以下、受信側制御手段２１は、光子検出器１８、１９のいずれが発火したかをビット情報に変換して受信側データ処理手段２３に伝送する。

上記の１パルス当たりの量子通信を、あらかじめ定めた回数だけ繰り返した後、送信側データ処理手段２２および受信側データ処理手段２３は、量子伝送路（光ファイバ通信路１）を介して秘匿性を保って伝送された情報と、公開通信路２を介して伝送された情報とを用いて秘匿性情報を共有する。すなわち、第１および第２の乱数と、量子通信で伝送されたビット情報とから、公開通信路２を用いて、情報の一部を交換しつつ、秘匿性が保証されたランダムな情報を共有する。

次に、図４に示すフローチャートを参照しながら、図１に示したこの発明の実施の形態１による量子通信動作について、さらに具体的に説明する。

図４において、量子暗号通信装置の光子パルス（量子暗号）に関連した量子通信部の処理ステップは、光子発生ステップＳ１と、光パルス分離・合流ステップＳ２と、位相変調器１３を経由しない光路を選択する光路選択ステップＳ３と、量子受信装置２００から量子送信装置１００への量子通信用の光子供給（往路）ステップＳ４と、送信側での第１アッテネートステップＳ５と、第１ファラディー回転ステップＳ６と、第１送信側位相変調ステップＳ７と、第２受信側位相変調ステップＳ６ａと、第２ファラディー回転ステップＳ７ａと、第２アッテネートステップＳ８と、量子送信装置１００から量子受信装置２００への量子通信用

の光子伝送（復路）ステップＳ９と、受信側位相変調ステップＳ１０と、光子分離・合流・干渉ステップＳ１１と、光子検出ステップＳ１２とを含む。

まず、量子受信装置２００内の光子発生器４は、受信側制御手段２１の制御下で光子パルスを発生する。発生した光子パルスは、偏光子５により偏光ビームスプリッタ６のＰ偏光に相当する光子パルスのみが通過する。Ｐ偏光に偏波面が揃えられた光子パルスは、偏光ビームスプリッタ６を透過する（光子発生ステップＳ１）。なお、光子パルスは、例えばレーザーパルスのように、パルス当たりの光子数がポアソン分布に従うように発生されてもよく、単一光子源を用いて、パルス当たり単一光子として発生されてもよい。

偏光ビームスプリッタ６を透過した光子パルスは、ビームスプリッタ７、８およびミラー９、１０により構成される非対称マッハツェンダ干渉計に導かれる。非対称マッハツェンダ干渉計に導かれた光子パルスは、この非対称マッハツェンダ干渉計内において光路長の異なる２つの光路に分離された後、再度合流して出力されることにより、光路長に応じた時間差を有する２連光子パルスとなる（光パルス分離・合流ステップＳ２）。なお、この非対称マッハツェンダ干渉計内では偏波面が保持される構成となっている。

非対称マッハツェンダ干渉計から出力された２連光子パルスは、先行する参照光パルスと後続する信号光パルスとにより構成され、いずれの光子パルスも偏波面が偏光ビームスプリッタ１１、１２に対してＰ偏光となるように偏波面が揃っているので、偏光ビームスプリッタ１１および１２を透過する光路が選択される（光路選択ステップＳ３）。

偏光ビームスプリッタ１２を透過した２連光子パルスは、光ファイバ通信路１に導かれ、そのまま量子送信装置１００に伝送される（光子供給（往路）ステップＳ４）。このとき、光ファイバ通信路１が有する複屈折性の揺らぎにより、２連光子パルスの偏波面は完全にランダムな状態になってしまう。

量子送信装置１００に導かれた２連光子パルスは、アッテネータ１４を透過することによって、パルス当たりの光子数が減衰された後、偏光ビームスプリッタ１５に導かれる（第１アッテネートステップＳ５）。

また、量子送信装置１００に導入された２連光子パルスは、各偏波面がランダ

ムなので、偏光ビームスプリッタ１５において、時計回りで周回する光子パルスと反時計回りで周回する光子パルスとに分離された後、再び偏光ビームスプリッタ１５で合流して２連光子パルスに戻る。

すなわち、２連光子パルスのうちの反時計回りの光子パルスは、光路ループ内において、ファラディー回転子１６および位相変調器１７の順に通過し、ファラディー回転子１６を通るときに、偏波面が非相反的に直角に回転させられる（第１ファラディー回転ステップＳ６）

また、反時計回りの光子パルスは、ファラディー回転子１６を通過した後、位相変調器１７に導入され、位相変調器１７を通過する際に、信号光パルスに当たる光子パルスのみが位相変調を受ける（第１送信側位相変調ステップＳ７）。

このときの位相変調の大きさは、送信側制御手段２０により制御され、送信側データ処理手段２２が出力した第１の乱数に応じて、制御信号通信路３を介して、同期タイミングを調整しつつ位相変調をかけることによって決定される。

一方、量子送信装置１００に導入された２連光子パルスのうち、時計回りの光子パルスの場合は、光路ループ内において、位相変調器１７およびファラディー回転子１６の順に通過するので、先に第２送信側位相変調ステップＳ６ａを経た後に、第２ファラディー回転ステップＳ７ａが実行される。なお、ファラディー回転子（非相反素子）１６による非相反的な偏波面の回転とは、回転の向きが光子パルスの進行方向に依存しないことを意味する。

また、光路ループ内の位相変調器１７において、反時計回りの光子パルスおよび時計回りの光子パルスのいずれに対しても、信号光パルスのみに対して選択的に位相変調をかけるためには、偏光ビームスプリッタ１５、ファラディー回転子１６および位相変調器１７を含む光路ループの光路長を、入射される２連光子パルスの時間差に相当する距離に比べて十分に短く設定すればよく、容易に実現することができる。

偏光ビームスプリッタ１５を介して、再び２連光子パルスに戻った光子パルスは、アッテネータ１４を再度通過する。このとき、信号光パルスの光子数が「１」を越えない程度まで、パルス当たりの光子レベル強度が減衰された後、光ファイバ通信路１に導入される（第２アッテネートステップＳ８）。

光ファイバ通信路１に再入射した２連光子パルスは、量子受信装置２００に向かって帰還することになるが、このとき、２連光子パルスの偏波状態は、光ファイバ通信路１の有する複屈折性の揺らぎによって、再びランダムな変動を受ける。

しかし、光ファイバ通信路１に再入射した２連光子パルスの偏波面は、量子送信装置１００内のファラディー回転子１６により、非相反的に直角に回転を受けているので、光ファイバ通信路１の往路上で受けた偏波変動と、復路上で受けた偏波変動が丁度打ち消し合うように作用する。

従って、再導入された２連光子パルスが量子受信装置２００内の偏光ビームスプリッタ１２に到達する時点では、２連光子パルスの偏波面は、偏光ビームスプリッタ１２から量子送信装置１００に向かった往路時と比べて、正確に直角に回転している（光子伝送（復路）ステップＳ９）。

このように、量子受信装置２００に到達した２連光子パルスは、偏波面が直角に回転した、偏光ビームスプリッタ１２にとってＳ偏光にあたる偏波面でもって、偏光ビームスプリッタ１２に導かれるので、偏光ビームスプリッタ１２において完全に反射され、位相変調器１３のある迂回光路に導かれる。２連光子パルスが位相変調器１３を通過する際に、参照光パルスのみが位相変調を受ける（受信側位相変調ステップＳ１０）。このときの位相変調の大きさは、受信側制御手段２１により制御され、受信側データ処理手段２３が出力した第２の乱数に応じて、位相変調の大きさが決定される。

２連光子パルスは位相変調器１３を通過後、偏光ビームスプリッタ１１で完全に反射されて、ビームスプリッタ８、７およびミラー１０、９により構成される往路で通過した非対称マッハツェンダ干渉計に再度導かれる。

非対称マッハツェンダ干渉計に再導入された２連光子パルスは、前述と同様に、それぞれ光路長の異なる２つの光路に分離された後、再度合流するまで、４つの光子パルスに分かれることになる。

すなわち、非対称マッハツェンダ干渉計に導入された２連光子パルスのうち、参照光パルスは、ビームスプリッタ８からビームスプリッタ７に直行する参照光先行光子パルスと、ミラー１０、９を通過する参照光後続光子パルスとに分離さ

れる。

同様に、信号光パルスは、ビームスプリッタ８からビームスプリッタ７に直行する信号光先行光子パルスと、ミラー１０、９を通過する信号光後続光子パルスとに分離される。

上記４つの光子パルスは、ビームスプリッタ７で再び合流するが、光路長差により時間差が生じしている。

但し、往路で通過した非対称マッハツェンダ干渉計を復路で再び通過するため、時間差が自動的に完全に一致する参照光後続光子パルスと信号光先行光子パルスは、ビームスプリッタ７に同時に到達し、干渉を引き起こすことになる（光子分離・合流・干渉ステップＳ１１）。

ビームスプリッタ７における干渉の結果、参照光後続光子パルスおよび信号光先行光子パルスの合流光子パルスは、光子検出器１８または１９のいずれかの一方に排他的に導かれることになる。

なお、光子検出器１９のある光路に導かれた光子パルスは、偏波面が往路のときと比べて直角に回転しているので、偏光ビームスプリッタ６で完全に反射されて、光子検出器１９に導かれる。

合流光子パルスが光子検出器１８、１９のどちらかに導かれるかは、第１送信側位相変調ステップＳ７において信号光パルスが受けた位相変調と、受信側位相変調ステップＳ１０において参照光パルスが受けた位相変調との位相差により確率的に決定される。但し、上記位相差が「０」または「π」の場合には、合流光子パルスの導かれる光子検出器が確定する。

このようにして、光子検出器１８、１９には、参照光先行光子パルスと、合流光子パルス（参照光後続光子パルスおよび信号光先行光子パルス）と、信号光後続光子パルスとがそれぞれ導かれる。

ここで、タイミングを調整することにより、合流光子パルスが導かれたときのみに、光子検出器１８、１９の一方を発火させることができる。

または、光子検出器１８、１９のいずれが発火してもよいが、受信側制御手段２１により、合流光子パルスが導かれたタイミングの発火のみを有効とすることができる。

いずれにせよ、受信側制御手段２１は、光子検出器１８、１９のどちらかが発火したことにより、「０」または「１」の量子通信ビット情報を定め、この量子通信ビット情報を受信側データ処理手段２３に送る（光子検出ステップＳ１２）。

以上が量子通信部の光子パルス当たりの動作フローである。

上記量子通信動作は、予め定めた回数だけ繰り返し実行され、その後、送信側データ処理手段２２および受信側データ処理手段２３は、公開通信路２を用いて相互に情報交換をしつつ、第１および第２の乱数と量子通信ビット情報から、秘匿性が保証されたランダムな情報を共有する。

このように、量子受信装置２００内において、非対称マッハツェンダ干渉計から出力されて、再び、同一の非対称マッハツェンダ干渉計に導入される光子パルスは、光ファイバ通信路１の有する任意の複屈折性揺らぎに起因してランダムな偏波変動が生じても、光ファイバ通信路１の送信側端（量子送信装置１００内のファラディー回転子１６）で非相反的に直角に偏波面が回転されて往復することにより、ランダムな偏波変動が打ち消されることになる。

従って、非対称マッハツェンダ干渉計に再導入された光子パルスは、偏波面が自動的に完全に整えられているので、偏波無依存性が要求されることは全くなく、偏波依存性を有していたとしても、光子パルスの偏波面の調整が全く不要となる。

また、往路において光子パルスを２連光子パルスに分離するために用いた非対称マッハツェンダ干渉計と、復路において、２連光子パルスを合流・干渉させるために用いた非対称マッハツェンダ干渉計に同一のものを用いているため、光路長差の調整が全く不要であり、かつ、光路長揺らぎに対しても自動的に補償されるような構成となり、安定な干渉系を構成することができる。

また、量子受信装置２００内の光路において、位相変調器１３を通る迂回光路を設け、上記のような量子送信装置１００内で偏波面が直角に回転されることを利用して、量子受信装置２００内で、光子発生器４から光ファイバ通信路１に向かう往路においては、光子パルスが位相変調器１３の無い光路を自動的に選択し、光ファイバ通信路１から光子検出器１８、１９に向かう復路においては、光子

パルスが位相変調器１３のある迂回光路を自動的に選択するようにしたことで、位相変調器１３において光子パルスの流れは一方向に限定され、光子パルスに不適切な位相変調がかけられるおそれが全くなくなり、光子パルス発生の繰り返し周波数を自由に選択することができる。

実施の形態２.

上述した実施の形態１では、２連光子パルスの偏波面が揃っているため、偏光ビームスプリッタ１１、１２のみで位相変調器１３を配置する迂回光路を実現したが、この実施の形態２では、特許文献１及び３、非特許文献１に記載された光学系のように、２連光子パルスの偏波面が揃っていない場合に、偏光ビームスプリッタと偏光変調器を用いて、位相変調器を配置した迂回光路を実現する場合を示す。

図５は、量子受信装置２００内に偏光変調器９を設けたこの発明の実施の形態２に係る量子暗号通信装置を示す構成図である。図５において、量子送信装置１００は、特許文献３に記載された光学系と類似の構成を有しており、光ファイバ通信路１に一端が接続されたアッテネータ１４と、アッテネータ１４の他端の光路に接続された偏光ビームスプリッタ１５と、偏光ビームスプリッタ１５のＰ偏光出力ポートに接続された偏光ビームスプリッタ４６と、偏光ビームスプリッタ４６の合波光入力ポートに接続されたファラディーミラー４７と、偏光ビームスプリッタ１５、４６のＳ偏光出力ポートに両端が接続された位相変調器１７と、位相変調器１７を制御する送信側制御手段２０と、送信側制御手段２０に接続されて第１の乱数を出力する送信側データ処理手段２２とを備えている。

偏光ビームスプリッタ１５、４６、ファラディーミラー４７、位相変調器１７は、量子通信用の光子パルスに対する両回転方向の光路ループを構成している。

量子送信装置１００は、量子受信装置２００から導入された光子パルスを、光ファイバ通信路１およびアッテネータ１４を介してファラディーミラー４７に導入し、非相反的に偏波面を回転・反射した後、再度アッテネータ１４および光ファイバ通信路１を介して量子受信装置２００に向けて反射するようになっている。

量子受信装置２００は、光子発生器４と、光子発生器４の出力光路に接続されたサーキュレータ４８と、サーキュレータ４８の他端にＰ偏光出力ポートが接続された偏光ビームスプリッタ６と、サーキュレータ４８のもう一端に接続された光子検出器１９と、偏光ビームスプリッタ６の合波光入力ポートに接続された半波長板４９と、偏光ビームスプリッタ６のＳ偏光出力ポートに接続された光子検出器１８と、半波長板４９にＰ偏光出力ポートが接続された２×２偏光ビームスプリッタ５０と、偏光ビームスプリッタ５０のＳ偏光出力ポートと対向するもう１つのポートを短絡するループ状光路と、偏光ビームスプリッタ５０の合波光入力ポートと接続する偏光変調器５１と、偏光変調器５１に合波光入力ポートが接続された偏光ビームスプリッタ１１と、偏光ビームスプリッタ１１のＳ偏光出力ポートに接続された位相変調器１３と、偏光ビームスプリッタ１１のＰ偏光出力ポートにＰ偏光出力ポートが接続され、かつ、位相変調器１３の他端がＳ偏光出力ポートに接続され、かつ、合波光入力ポートが光ファイバ通信路１に接続された偏光ビームスプリッタ１２と、光子検出器１８、１９の検出信号を取り込み、かつ、偏光変調器５１と位相変調器１３と光子検出器１８、１９と光子発生器４を制御する受信側制御手段２１と、受信側制御手段２１に接続されて第２の乱数を出力し、光子検出信号を入力する受信側データ処理手段２３とを備えている。

量子受信装置２００内の偏光ビームスプリッタ１２は、光ファイバ通信路１を介して量子送信装置１００内のアッテネータ１４に接続され、受信側制御手段２１は、制御信号通信路３を介して送信側制御手段２０に接続され、受信側データ処理手段２３は、公開通信路２を介して送信側データ処理手段２２に接続されている。

量子受信装置２００内において、偏光ビームスプリッタ５０から２連光子パルスが偏光変調器５１に向かって出力されるが、先行する参照光パルスはＰ偏光の偏波面を持っているのに対し、後続する信号光パルスはＳ偏光の偏波面を持っている。このため、偏光変調器５１が通過する信号光パルスのみ偏波面を直角に回転し、量子受信装置２００から量子送信装置１００へ伝送する際には、２連光子パルスをＰ偏光に偏波面を揃えて、偏光ビームスプリッタ１１、１２を透過させる。

Ｓ偏光した２連光子パルスが量子送信装置１００から量子受信装置２００へ帰還した際には、偏光ビームスプリッタ１２で反射され位相変調器１３を経由する光路が選択される。位相変調器１３を通過した２連光子パルスは、偏光ビームスプリッタ１１で反射され、偏光変調器５１を通過する、２連光子パルスが偏光変調器５１を通過する際、偏光変調器５１は、信号光パルスのみ偏波面を直角に回転し、Ｐ偏光の偏波面にする。このため、偏光ビームスプリッタ５０で参照光パルスは完全に反射されてループ状光路を経た後、半波長板４９に向かい、信号光パルスは、偏光ビームスプリッタ５０を透過し半波長板４９に直行することになる。

次に、図５に示したこの発明の実施の形態２に係る量子暗号通信装置の動作について説明する。

受信側制御手段２１は、制御信号通信路３を介した制御信号の相互通信により、量子送信装置１００内の送信側制御手段２０と同期・調歩動作する。量子受信装置２００内の光子発生器４は、受信側制御手段２１が出力する同期信号に応じて、偏波面の揃った光子パルスを発生する。

光子発生器４から発生した光子パルスは、サーキュレータ４８を経て偏光ビームスプリッタ６に入光する。なお、光子パルスは偏光ビームスプリッタ６のＰ偏光に偏波面が揃っているとする。

光子パルスは、偏光ビームスプリッタ６を透過し、半波長板４９に導かれる。半波長板４９によって、偏波面が４５度回転させられた後、偏光ビームスプリッタ５０に入光する。光子パルスは偏波面が４５度傾いているため、Ｐ偏光である参照光パルスとＳ偏光である信号光パルスの２つの光子パルスに分離される。信号光パルスは、ループ状光路を経た後、偏光ビームスプリッタ５０の偏光変調器５１に接続する合波光出力ポートから出力され、先行する参照光パルスと後続する信号光パルスからなる２連光子パルスが偏光変調器５１に導かれる。

偏光変調器５１に導かれた２連光子パルスのうち、Ｓ偏光である信号光パルスは偏光変調器５１により偏波面を直角に回転させられ、Ｐ偏光になる、このため、偏光変調器５１を通過後、偏光ビームスプリッタ１１に導かれた２連光子パルスは、偏光ビームスプリッタ１１、１２をこの順に通過し、位相変調器１３のあ

る迂回光路に導かれることなく、光ファイバ通信路１に導かれる。

なお、図５における量子受信装置２００の光学系の構成例としては種々採用できる。図６Ａは、図５に示す量子受信装置２００において、１つの光子パルスから２連光子パルスに分離・出力するための光学系の構成例であり、１×２偏光ビームスプリッタ６と、半波長板４９と、２×２偏光ビームスプリッタ５０と、ループ状光路を用い、位相変調器用迂回光路の構成例として、偏光変調器５１と、１×２タイプの偏光ビームスプリッタ１１、１２との２個を用いた構成例を示したが、図６Ｂに示すように、１×２タイプの偏光ビームスプリッタ５２、５３の２式用いた２連光子パルス分離・出力光学系の構成例や、図６Ｃに示すように、２×２偏光ビームスプリッタ５４を１式用いた迂回光路の構成例や、図６Ｄに示すように、ビームスプリッタ５５と、偏光コントローラ５６と、ミラー５７、５８と、偏光ビームスプリッタ５９を用いた２連光子パルス分離・出力光学系の構成例や、図６Ｅに示すように、カプラ６０と、遅延ファイバ６１と、偏光コントローラ６２と、偏光ビームスプリッタ６３とを用いた２連光子パルス分離・出力光学系の構成例も存在し、特定の１つの構成例に特化されるものではない。

量子受信装置２００から光ファイバ通信路１に導かれた２連光子パルスは、量子送信装置１００に導入され、量子送信装置１００内のファラディーミラー４７により偏波面を非相反的に直角に回転・反射させられ、位相変調器１７により信号光パルスが位相変調を受けた後、再び量子受信装置２００に帰還してくる。

なお、図５においては、量子送信装置１００の光学系の構成例として、アッテネータ１４と、偏光ビームスプリッタ１５、４６と、ファラディーミラー４７と、位相変調器１７を用いた構成例を示したが、実施の形態１と同様に、図３Ａ－図３Ｅに示したような構成例も存在し、特定の１つの構成例に特化されるものではない。

量子受信装置２００に帰還した２連光子パルスは、偏光ビームスプリッタ１２で完全に反射されて、位相変調器１３が配置された迂回光路に導かれる。なぜならば、光ファイバ通信路１の一方の端点で入射された光は、他方の端点で非相反的に直角に偏波面の回転を受けて反射して帰還する場合に、途中の光路でいかなる複屈折性の揺らぎが存在したとしても、入射した時点から直角に偏波面が回転

した状態で帰還するからである。

偏光ビームスプリッタ１２で反射された２連光子パルスは、位相変調器１３に入光する。このとき、位相変調器１３は、受信側制御手段２１の制御下で、受信側データ処理手段２３が出力した第２の乱数に応じて、参照光パルスのみに対して位相変調をかける。

位相変調器１３を通過した２連光子パルスは、偏光ビームスプリッタ１１で完全に反射されて偏光変調器５１へと導かれる。２連光子パルスが偏光変調器５１を通過する際、信号光パルスのみ偏波面を直角に回転させられ、Ｓ偏光からＰ偏光にかわる。

偏光変調器５１を通過した２連光子パルスは、偏光ビームスプリッタ５０に導入される。Ｓ偏光である参照光パルスは、偏光ビームスプリッタ５０において完全に反射させられて、ループ状光路を経た後、半波長板４９に導かれる。一方、Ｐ偏光である信号光パルスは、偏光ビームスプリッタ５０を透過し、半波長板４９に導かれる。

このとき、参照光パルスは、信号光パルスが量子受信装置２００から量子送信装置１００に向かう往路で通過したときと同一のループ状光路を通過するので、参照光パルスと信号光パルスの間の時間差は完全に打ち消されて、１つの光子パルスとして合流・干渉を引き起こすことになる。干渉を引き起こした光子パルスは、この干渉の場合は、偏波面が排他的に２つの直交する偏波面のいずれか１つとなる。

半波長板４９に導かれた、干渉を引き起こした光子パルスは、半波長板４９により偏波面を－４５度回転させられた後、偏光ビームスプリッタ６に導かれる。偏光ビームスプリッタ６に導かれた光子パルスは、干渉の結果、排他的に１対の光子検出器１８、１９のいずれかに接続する一方のポートに導かれ、一方の光子検出器を発火する。なお、光子検出器１９に接続するポートに導かれた光子パルスは、サーキュレータ４８により光子検出器１９に導かれることになる。

受信側制御手段２１は、光子検出器１８、１９のいずれが発火したかをビット情報に変換し、受信側データ処理手段２３に伝送する。

受信側データ処理手段２３は、第２の乱数と、量子情報で伝送されたビット情

報とから、公開通信路２を用いて、量子送信装置１００と情報の一部を交換しつつ、秘匿性が保証されたランダムな情報を共有する。

次に、量子送信装置１００に注目しながら、具体的な動作について説明する。

量子受信装置２００から光ファイバ通信路１を通過して量子送信装置１００に導入された２連光子パルスは、量子送信装置１００に到達した時点では、光ファイバ通信路１の有する複屈折性の揺らぎにより偏波面が完全にランダムな状態になっている。

この状態で、量子送信装置１００に導入された２連光子パルスは、アッテネータ１４で減衰された後、偏光ビームスプリッタ１５によりそれぞれ直交する２つの偏波モード（Ｐ偏光とＳ偏光）に分離される。

このようにして、４つに分離された光子パルスのうち、時計回りに進行する２連光子パルス（Ｓ偏光）は、偏光ビームスプリッタ１５で反射され、位相変調器１７を通過した後、偏光ビームスプリッタ４６で反射され、ファラディーミラー４７に導かれる。ファラディーミラー４７で非相反的に偏波面を直角に回転・反射させられた後、偏光ビームスプリッタ４６を透過し、偏光ビームスプリッタ１５に戻る。

また、４つに分離された光子パルスのうち、反時計回りに進行する２連光子パルス（Ｐ偏光）は、偏光ビームスプリッタ１５、４６を通過し、ファラディーミラー４７で非相反的に偏波面を直角に回転・反射させられ、偏光ビームスプリッタ４６で反射され、位相変調器１７を通過した後、偏光ビームスプリッタ１５に戻る。

このとき、位相変調器１７は、送信側制御手段２０の制御下で、送信側制御手段２２が出力した第１の乱数に応じて、２連光子パルスのうち信号光パルスのみに対して、時計回りまたは反時計回りの進行方向に依存することなく、位相変調器１７を通過する際に位相変調をかけている。

偏光ビームスプリッタ１５に戻った４つの光子パルスは、分離合流するまでの光路長が、時計回りまたは反時計回りに依存せずに等しいので、再び２連光子パルスとなり、アッテネータ１４に導入される。ここで、アッテネータ１４の光子レベル強度の減衰の大きさは、信号光パルスの光子数が「１」を越えない強度と

なるように調整されている。

このようにして、再び光ファイバ通信路１に導入されて量子受信装置２００に帰還した２連光子パルスは、前述したとおり、偏光ビームスプリッタ１２により完全に反射されて、位相変調器１３のある迂回光路を通った後、偏光ビームスプリッタ１１で反射されて、光子検出器１８、１９の設置されたポートに導かれる。

以下、受信側制御手段２１は、光子検出器１８、１９のいずれが発火したかをビット情報に変換して受信側データ処理手段２３に伝送する。

上記の１パルス当たりの量子通信を、あらかじめ定めた回数だけ繰り返した後、送信側データ処理手段２２および受信側データ処理手段２３は、量子伝送路（光ファイバ通信路１）を介して秘匿性を保って伝送された情報と、公開通信路２を介して伝送された情報とを用いて秘匿性情報を共有する。すなわち、第１および第２の乱数と、量子通信で伝送されたビット情報とから、公開通信路２を用いて、情報の一部を交換しつつ、秘匿性が保証されたランダムな情報を共有する。

次に、図７に示すフローチャートを参照しながら、図５に示したこの発明の実施の形態２による量子通信動作について、さらに具体的に説明する。

図７において、量子暗号通信装置の光子パルス（量子暗号）に関連した量子通信部の処理ステップは、光子発生ステップＳ１と、光パルス分離・合流ステップＳ２と、信号光パルスの偏波面を回転させる第１偏波回転ステップＳ３と、位相変調器１３のない光路を選択する光路選択ステップＳ４と、量子受信装置２００から量子送信装置１００への量子通信用の光子供給（往路）ステップＳ５と、送信側での第１アッテネートステップＳ６と、第１ファラディー回転反射ステップＳ７と、第１送信側位相変調ステップＳ８と、第２送信側位相変調ステップＳ７ａと、第２ファラディー回転反射ステップＳ８ａと、第２アッテネートステップＳ９と、量子送信装置１００から量子受信装置２００への量子通信用の光子伝送（復路）ステップＳ１０と、受信側位相変調ステップＳ１１と、再び信号光パルスの偏波面を回転させる第２偏波回転ステップＳ１２と、光子分離・合流・干渉ステップＳ１３と、光子検出ステップＳ１４とを含む。

まず、量子受信装置２００内の光子発生器４は、受信側制御手段２１の制御下

で光子パルスを発生する。発生した光子パルスは、サーキュレータ４８により偏光ビームスプリッタ６に導かれる。光子パルスは、Ｐ偏光に偏波面が揃えられている（光子発生ステップＳ１）。なお、光子パルスは、例えばレーザーパルスのように、パルス当たりの光子数がポアソン分布に従うように発生されてもよく、単一光子源を用いて、パルス当たり単一光子として発生されてもよい。

偏光ビームスプリッタ６に導かれた光子パルスは、偏光ビームスプリッタ６を透過し、半波長板４９に導かれ、偏波面を４５度回転させられる。偏波面を４５度回転させられた光子パルスは、偏光ビームスプリッタ５０に導かれ、Ｐ偏光である参照光パルスとＳ偏光である信号光パルスに分離される。信号光パルスは、ループ上光路を経た後、参照光パルスと合流して、２連光子パルスとして偏光変調器５１に向かって出力される（光パルス分離・合流ステップＳ２）。

偏光変調器５１に導かれた２連光子パルスは、信号光パルスのみ偏波面を直角に回転させられて、偏波面の揃った２連光子パルスとなる（第１偏波回転ステップＳ３）。

偏光変調器５１から出力された２連光子パルスは、参照光パルスと信号光パルスのいずれの光子パルスも偏波面が偏光ビームスプリッタ１１、１２に対してＰ偏光となるように偏波面が揃っているので、偏光ビームスプリッタ１１および１２を透過する光路が選択される（光路選択ステップＳ４）。

偏光ビームスプリッタ１２を透過した２連光子パルスは、光ファイバ通信路１に導かれ、そのまま量子送信装置１００に伝送される（光子供給（往路）ステップＳ５）。このとき、光ファイバ通信路１が有する複屈折性の揺らぎにより、２連光子パルスの偏波面は完全にランダムな状態になってしまう。

量子送信装置１００に導かれた２連光子パルスは、アッテネータ１４を透過することによって、パルス当たりの光子数が減衰された後、偏光ビームスプリッタ１５に導かれる（第１アッテネートステップＳ６）。

また、量子送信装置１００に導入された２連光子パルスは、各偏波面がランダムなので、偏光ビームスプリッタ１５において、時計回りで周回する光子パルスと反時計回りで周回する光子パルスとに分離された後、再び偏光ビームスプリッタ４６で合流して２連光子パルスに戻る。

すなわち、２連光子パルスのうちの反時計回りの光子パルスは、光路ループ内において、偏光ビームスプリッタ４６、ファラディーミラー４７、偏光ビームスプリッタ４６および位相変調器１７の順に通過し、ファラディーミラー４７を通るときに、偏波面が非相反的に直角に回転・反射させられる（第１ファラディー回転反射ステップＳ７）。

また、反時計回りの光子パルスは、ファラディーミラー４７で反射された後、位相変調器１７に導入され、位相変調器１７を通過する際に、信号光パルスに当たる光子パルスのみが位相変調を受ける（第１送信側位相変調ステップＳ８）。

このときの位相変調の大きさは、送信側制御手段２０により制御され、送信側データ処理手段２２が出力した第１の乱数に応じて、制御信号通信路３を介して、同期タイミングを調整しつつ位相変調をかけることによって決定される。

一方、量子送信装置１００に導入された２連光子パルスのうち、時計回りの光子パルスの場合は、光路ループ内において、位相変調器１７およびファラディーミラー４７の順に通過するので、先に第２送信側位相変調ステップＳ７ａを経た後に、第２ファラディー回転反射ステップＳ８ａが実行される。なお、ファラディーミラー（非相反素子）４７による非相反的な偏波面の回転とは、回転の向きが光子パルスの進行方向に依存しないことを意味する。

また、光路ループ内の位相変調器１７において、反時計回りの光子パルスおよび時計回りの光子パルスのいずれに対しても、信号光パルスのみに対して選択的に位相変調をかけるためには、偏光ビームスプリッタ１５、４６、ファラディーミラー４７および位相変調器１７を含む光路ループの光路長を、入射される２連光子パルスの時間差に相当する距離に比べて十分に短く設定すればよく、容易に実現することができる。

偏光ビームスプリッタ１５を介して、再び２連光子パルスに戻った光子パルスは、アッテネータ１４を再度通過する。このとき、信号光パルスの光子数が「１」を越えない程度まで、パルス当たりの光子レベル強度が減衰された後、光ファイバ通信路１に導入される（第２アッテネートステップＳ９）。

光ファイバ通信路１に再入射した２連光子パルスは、量子受信装置２００に向かって帰還することになるが、このとき、２連光子パルスの偏波状態は、光ファ

イバ通信路１の有する複屈折性の揺らぎによって、再びランダムな変動を受ける。

しかし、光ファイバ通信路１に再入射した２連光子パルスの偏波面は、量子送信装置１００内のファラディーミラー４７により、非相反的に直角に回転を受けているので、光ファイバ通信路１の往路上で受けた偏波変動と、復路上で受けた偏波変動が丁度打ち消し合うように作用する。

従って、再導入された２連光子パルスが量子受信装置２００内の偏光ビームスプリッタ１２に到達する時点では、２連光子パルスの偏波面は、偏光ビームスプリッタ１２から量子送信装置１００に向かった往路時と比べて、正確に直角に回転している（光子伝送（復路）ステップＳ１０）。

このように、量子受信装置２００に到達した２連光子パルスは、偏波面が直角に回転した、偏光ビームスプリッタ１２にとってＳ偏光にあたる偏波面でもって、偏光ビームスプリッタ１２に導かれるので、偏光ビームスプリッタ１２において完全に反射され、位相変調器１３のある迂回光路に導かれる。２連光子パルスが位相変調器１３を通過する際に、参照光パルスのみが位相変調を受ける（受信側位相変調ステップＳ１１）。このときの位相変調の大きさは、受信側制御手段２１により制御され、受信側データ処理手段２３が出力した第２の乱数に応じて、位相変調の大きさが決定される。

２連光子パルスは、位相変調器１３を通過後、偏光ビームスプリッタ１１で完全に反射されて、偏光変調器５１に導かれる。

偏光変調器５１に導入された２連光子パルスは、偏光変調器５１を通過する際、信号光パルスのみ偏波面を直角に回転させられ、Ｓ偏光からＰ偏光となる（第２偏波回転ステップＳ１２）。

偏光変調器５１から偏光ビームスプリッタ５０に導かれた２連光子パルスは、参照光パルスが偏光ビームスプリッタ５０で完全に反射され、ループ状光路を通る。信号光パルスは偏光ビームスプリッタ５０を透過する。従って、偏光ビームスプリッタ５０から出力される際、参照光パルスと信号光パルスは同時に出力され、合流して１つの光子パルスとなる。参照光パルスと信号光パルスが合流する際、干渉が引き起こされる。干渉の結果、偏波面が排他的に２つの直交する偏波

面のいずれか１つとなっている。

干渉を引き起こした光子パルスは、半波長板４９に導かれ、偏波面を－４５度回転させられる。偏波面を－４５度回転させられた干渉を引き起こした光子パルスは、偏波ビームスプリッタ６に導かれ、光子検出器１８、１９のあるいずれか一方のポートへ出力される（光子分離・合流・干渉ステップＳ１３）。干渉を引き起こした光子パルスは、光子検出器１８または１９のいずれかの一方に排他的に導かれることになる。

なお、光子検出器１９のある光路に導かれた光子パルスは、サーキュレータ４８により光子検出器１９に導かれる。

干渉を引き起こした光子パルスが光子検出器１８、１９のどちらかに導かれるかは、第１送信側位相変調ステップＳ８において信号光パルスが受けた位相変調と、受信側位相変調ステップＳ１１において参照光パルスが受けた位相変調との位相差により確率的に決定される。但し、上記位相差が「０」または「π」の場合には、干渉を引き起こした光子パルスの導かれる光子検出器が確定する。

受信側制御手段２１は、光子検出器１８、１９のどちらかが発火したことにより、「０」または「１」の量子通信ビット情報を定め、この量子通信ビット情報を受信側データ処理手段２３に送る（光子検出ステップＳ１４）。

以上が量子通信部の光子パルス当たりの動作フローである。

上記量子通信動作は、予め定めた回数だけ繰り返し実行され、その後、送信側データ処理手段２２および受信側データ処理手段２３は、公開通信路２を用いて相互に情報交換をしつつ、第１および第２の乱数と量子通信ビット情報から、秘匿性が保証されたランダムな情報を共有する。

このように、量子受信装置２００から出力されて、量子受信装置２００に再び導入される光子パルスは、光ファイバ通信路１の有する任意の複屈折性揺らぎに起因してランダムな偏波変動が生じても、光ファイバ通信路１の送信側端（量子送信装置１００内のファラディーミラー４７）で非相反的に直角に偏波面が回転・反射されて往復することにより、ランダムな偏波変動が打ち消されることになる。

従って、量子受信装置２００に再導入された光子パルスは、偏波面が自動的に

完全に整えられているので、偏波無依存性が要求されることは全くなく、偏波依存性を有していたとしても、光子パルスの偏波面の調整が全く不要となる。

また、往路において光子パルスを２連光子パルスに分離するために用いた光学系と、復路において、２連光子パルスを合流・干渉させるために用いた光学系に同一のものを用いているため、光路長差の調整が全く不要であり、かつ、光路長揺らぎに対しても自動的に補償されるような構成となり、安定な干渉系を構成することができる。

また、量子受信装置２００内の光路において、２連光子パルスの偏波面が揃っていない場合でも、一方の光子パルスのみに選択的に偏光変調をかけ偏波面を揃えること、位相変調器１３を通る迂回光路を設け、上記のような量子送信装置１００内で偏波面が直角に回転されることを利用して、量子受信装置２００内で、光子発生器４から光ファイバ通信路１に向かう往路においては、光子パルスが位相変調器１３の無い光路を自動的に選択し、光ファイバ通信路１から光子検出器１８、１９に向かう復路においては、光子パルスが位相変調器１３のある迂回光路を自動的に選択するようにしたことで、位相変調器１３において光子パルスの流れは一方向に限定され、光子パルスに不適切な位相変調がかけられるおそれが全くなくなり、光子パルス発生の繰り返し周波数を自由に選択することができる。

産業上の利用の可能性

以上のように、この発明によれば、偏波面制御は不要で、光路長揺らぎに安定し、かつ動作周波数が自由に選択できる量子暗号通信装置を実現できる。

請 求 の 範 囲

1． 量子を伝送するための量子通信路と、

前記量子伝送路の送信側に設置された量子送信装置と、

前記量子伝送路の受信側に設置された量子受信装置と、

前記量子送信装置と前記量子受信装置を結合して同期信号を含む制御信号を相互通信するための制御信号通信路と

を備えた量子暗号通信装置であって、

前記量子受信装置は、

量子源となる光源と、

前記光源から出た光子パルスから信号光パルスと参照光パルスとの時間差２連光子パルスを発生すると共に、逆進する量子である信号光パルスと参照光パルスとを合波、干渉させるための合波干渉手段を有するループ状光路と、

前記量子通信路との接続口に設けられて、前記時間差２連光子パルスが前記量子通信路を介して前記量子送信装置と前記量子受信装置との間を往復した後、受信される前記参照光パルスのみに対して位相変調をかける位相変調器を有する迂回光路と、

前記ループ状光路を介した干渉光を観測する光子検出器と

を含み、

前記量子送信装置は、

前記量子受信装置から前記量子通信路を介して到達した２連光子パルスの偏波面を非相反的に直角に回転させる偏波回転手段と、

前記偏波回転手段を通過した信号光パルスに位相変調をかけて再び量子通信路を通って前記量子受信装置に戻す位相変調器と、

信号光パルスをパルス中に光子が２個以上含まない状態まで減光する減光手段と

を含む

ことを特徴とする量子暗号通信装置。

2. 請求項１記載の量子暗号通信装置において、

前記迂回光路の送信光路と受信光路との分岐点に、前記２連光子パルスの前記信号光パルスと前記参照光パルスの偏波面が同じ場合、帰還光子パルスのみ前記位相変調器のある受信光路を通過させる偏光ビームスプリッタを設けた

ことを特徴とする量子暗号通信装置。

3. 請求項１記載の量子暗号通信装置において、

前記ループ状光路と前記迂回光路との間に、前記２連光子パルスの信号光パルスと参照光パルスの偏波面が異なる場合、信号光パルスが通過するときのみ偏波面を回転することで、往路での２連光子パルスの偏波面を揃える偏光変調器を設けた

ことを特徴とする量子暗号通信装置。

4. 請求項２または３に記載の量子暗号通信装置において、

前記偏光ビームスプリッタとして、１×２入出力型偏光ビームスプリッタを２式用い、特定の偏波面の光子パルスのみを前記位相変調器のある受信光路に導く

ことを特徴とする量子暗号通信装置。

5. 請求項２または３に記載の量子暗号通信装置において、

前記偏光ビームスプリッタとして、２×２入出力型偏光ビームスプリッタを１式用い、特定の偏波面の光子パルスのみを位相変調器のある受信光路に導く

ことを特徴とする量子暗号通信装置。

図 1

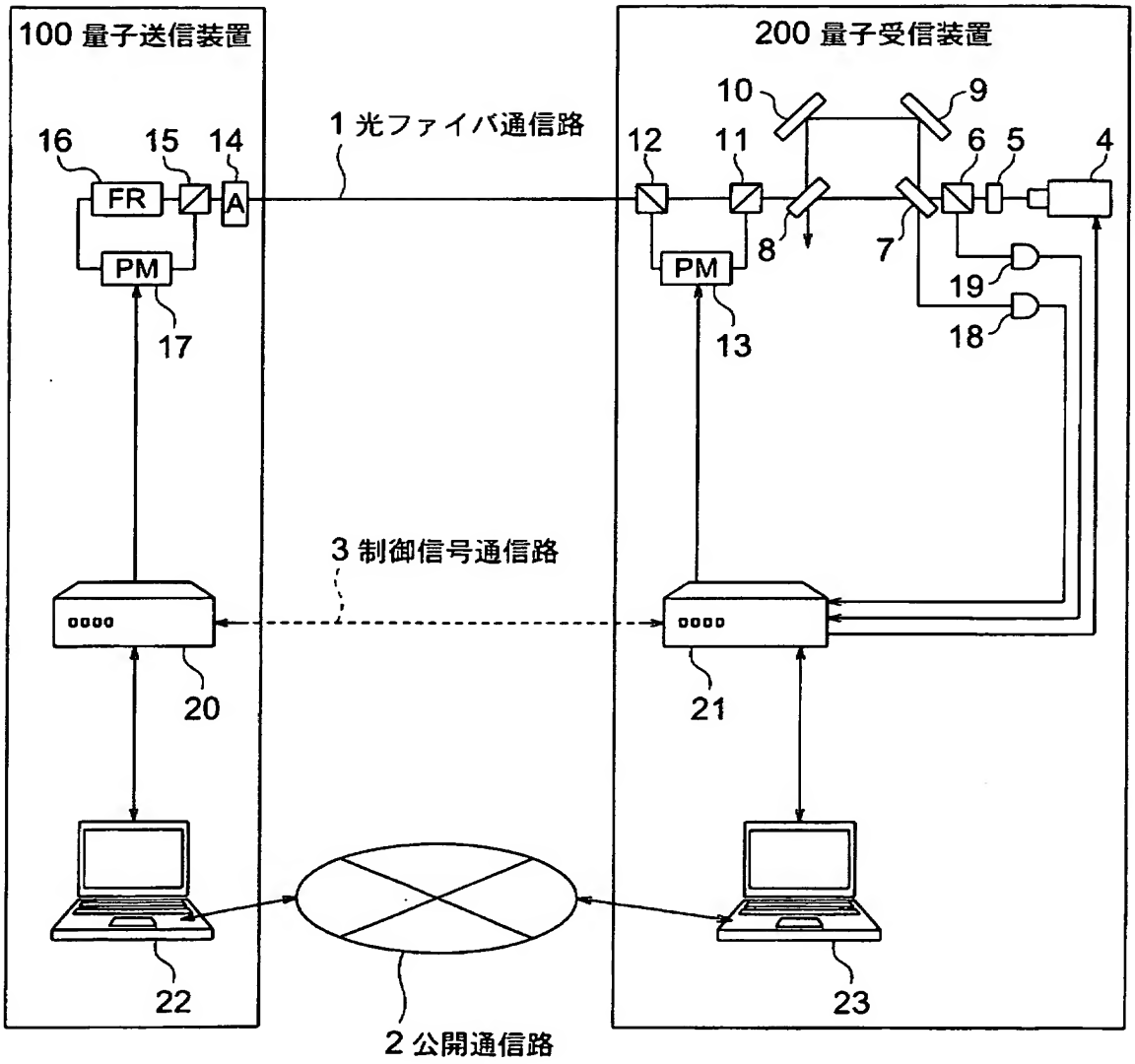

100 量子送信装置
200 量子受信装置
1 光ファイバ通信路
2 公開通信路
3 制御信号通信路
FR
A
PM
PM
16
15
14
17
10
9
12
11
6
5
4
8
7
19
18
13
20
21
22
23

図 2A

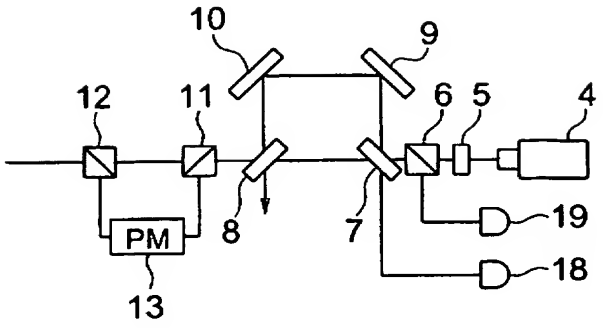


図 2B

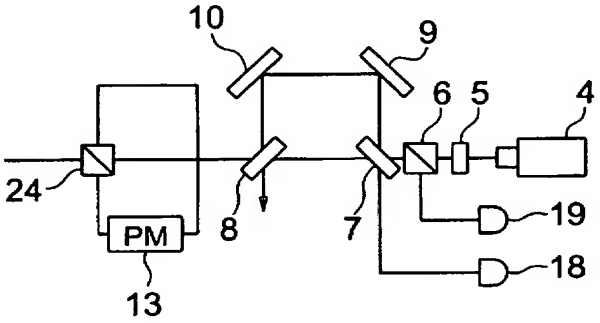


図 2C

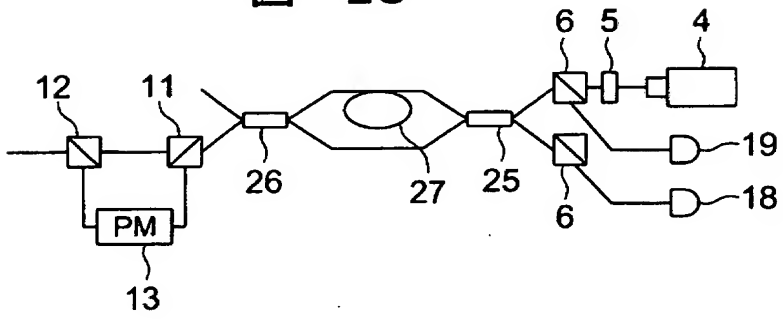


図 2D

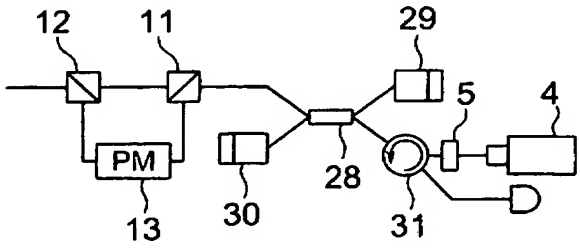


図 3A

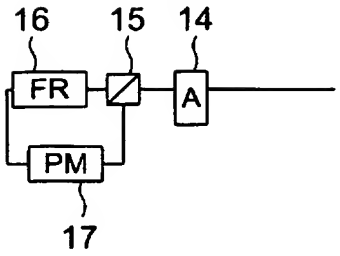


図 3B

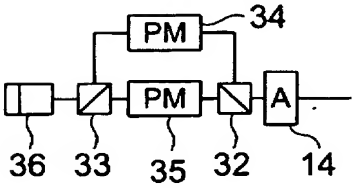


図 3C

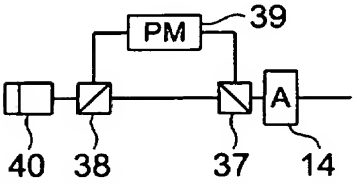


図 3D

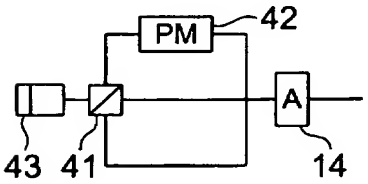


図 3E

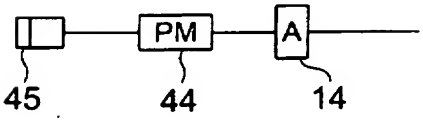


図 4

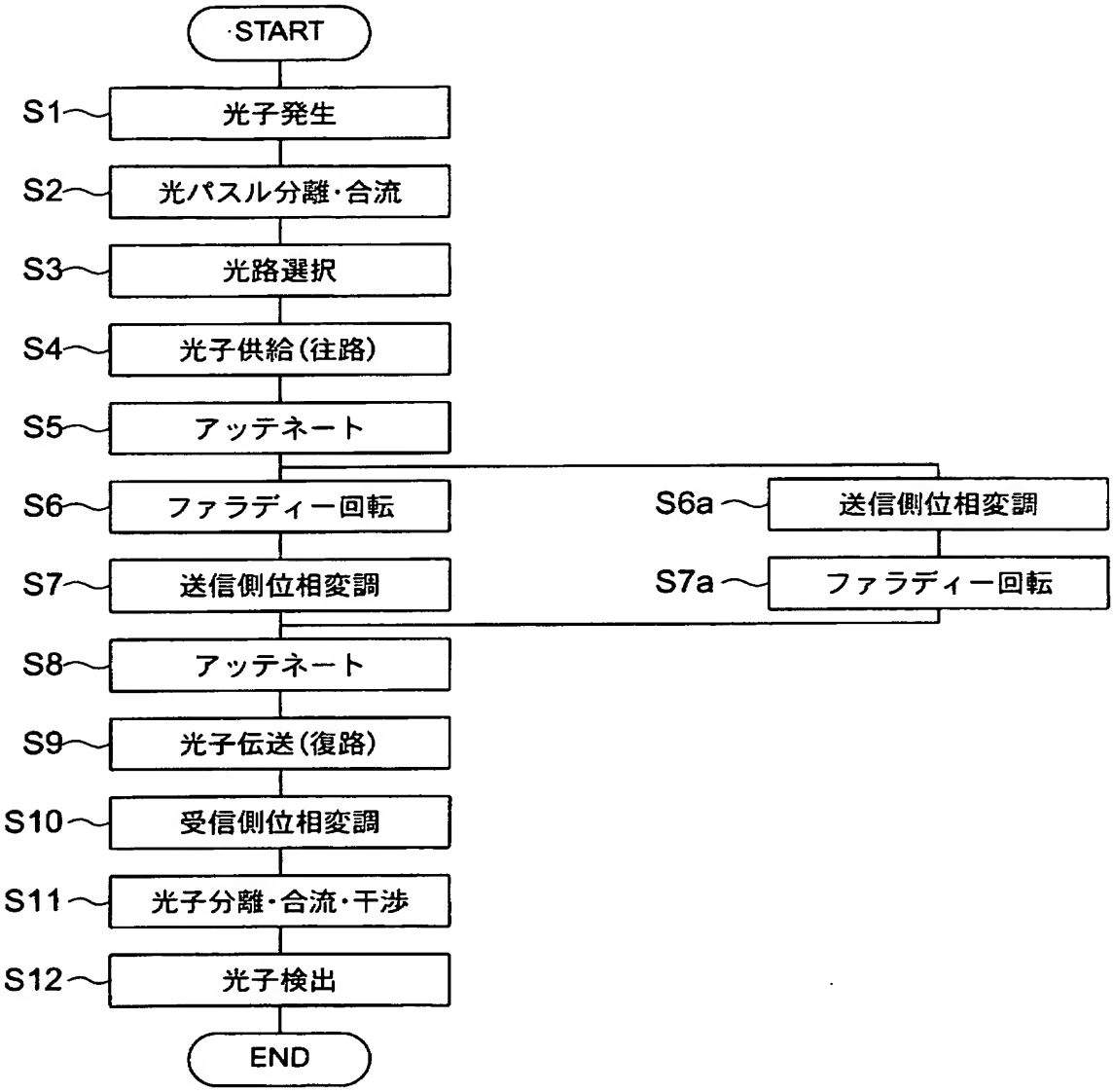

START
S1
光子発生
S2
光パスル分離・合流
S3
光路選択
S4
光子供給(往路)
S5
アッテネート
S6
ファラディー回転
S7
送信側位相変調
S6a
送信側位相変調
S7a
ファラディー回転
S8
アッテネート
S9
光子伝送(復路)
S10
受信側位相変調
S11
光子分離・合流・干渉
S12
光子検出
END

図 5

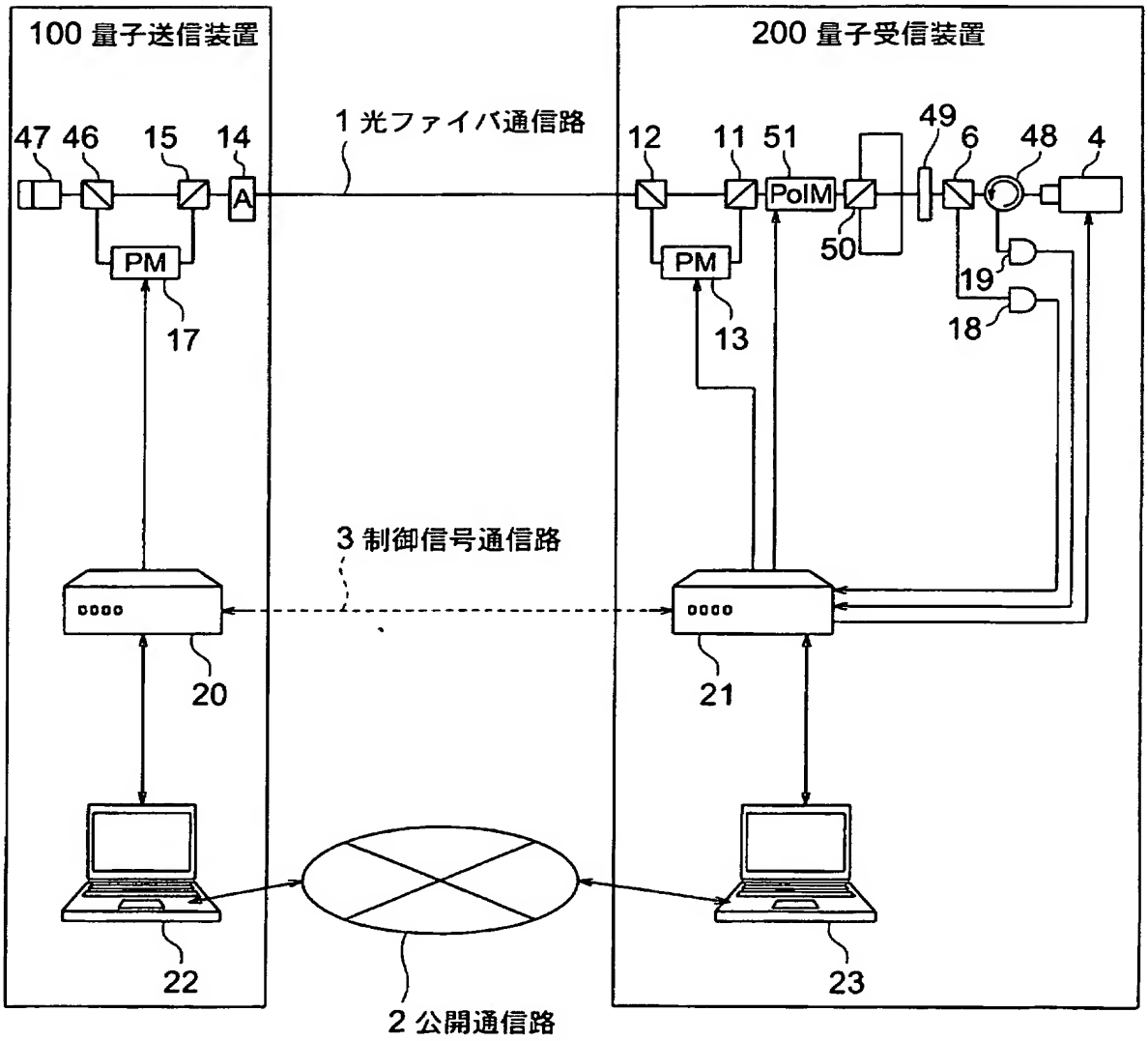

100 量子送信装置
200 量子受信装置
1 光ファイバ通信路
47
46
15
14
A
PM
17
12
11
51
PolM
49
6
48
4
50
19
18
PM
13
3 制御信号通信路
20
21
22
23
2 公開通信路

図 6A

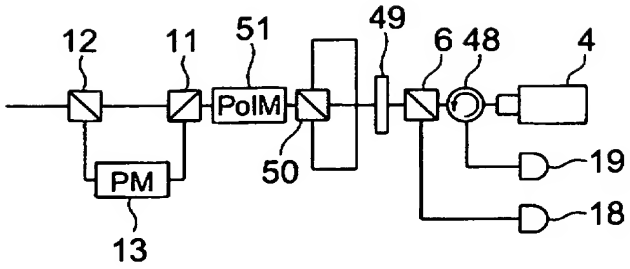

12
11
51
49
6
48
4
PolM
PM
50
19
18
13

図 6B

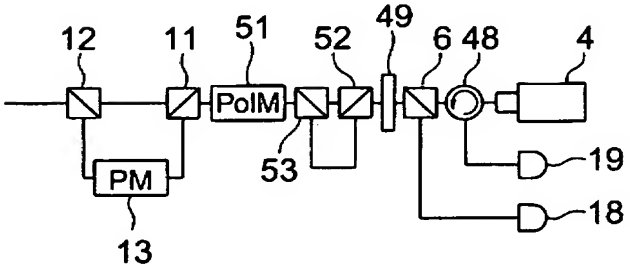

12
11
51
52
49
6
48
4
PolM
PM
53
19
18
13

図 6C

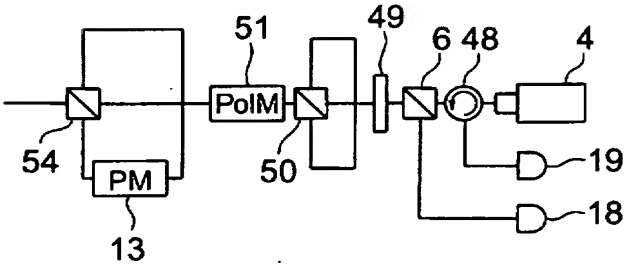

51
49
6
48
4
PolM
54
PM
50
19
18
13

図 6D

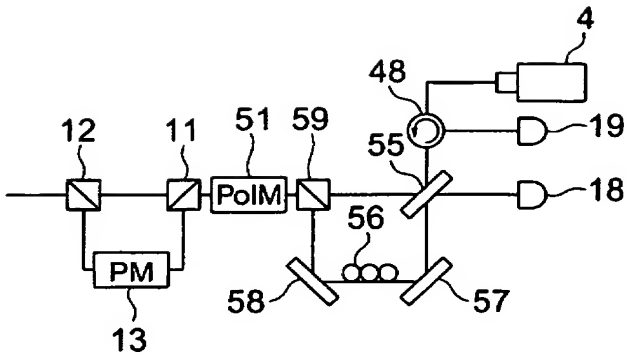

4
48
12
11
51
59
55
19
PolM
18
56
PM
58
57
13

図 6E

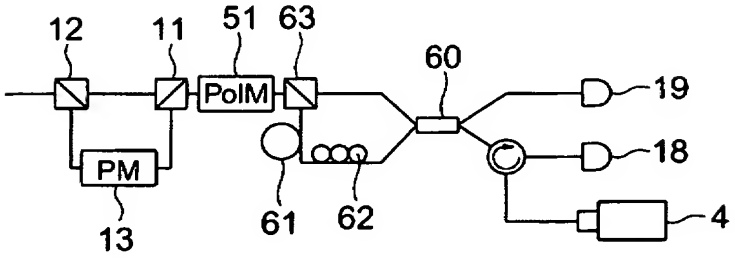
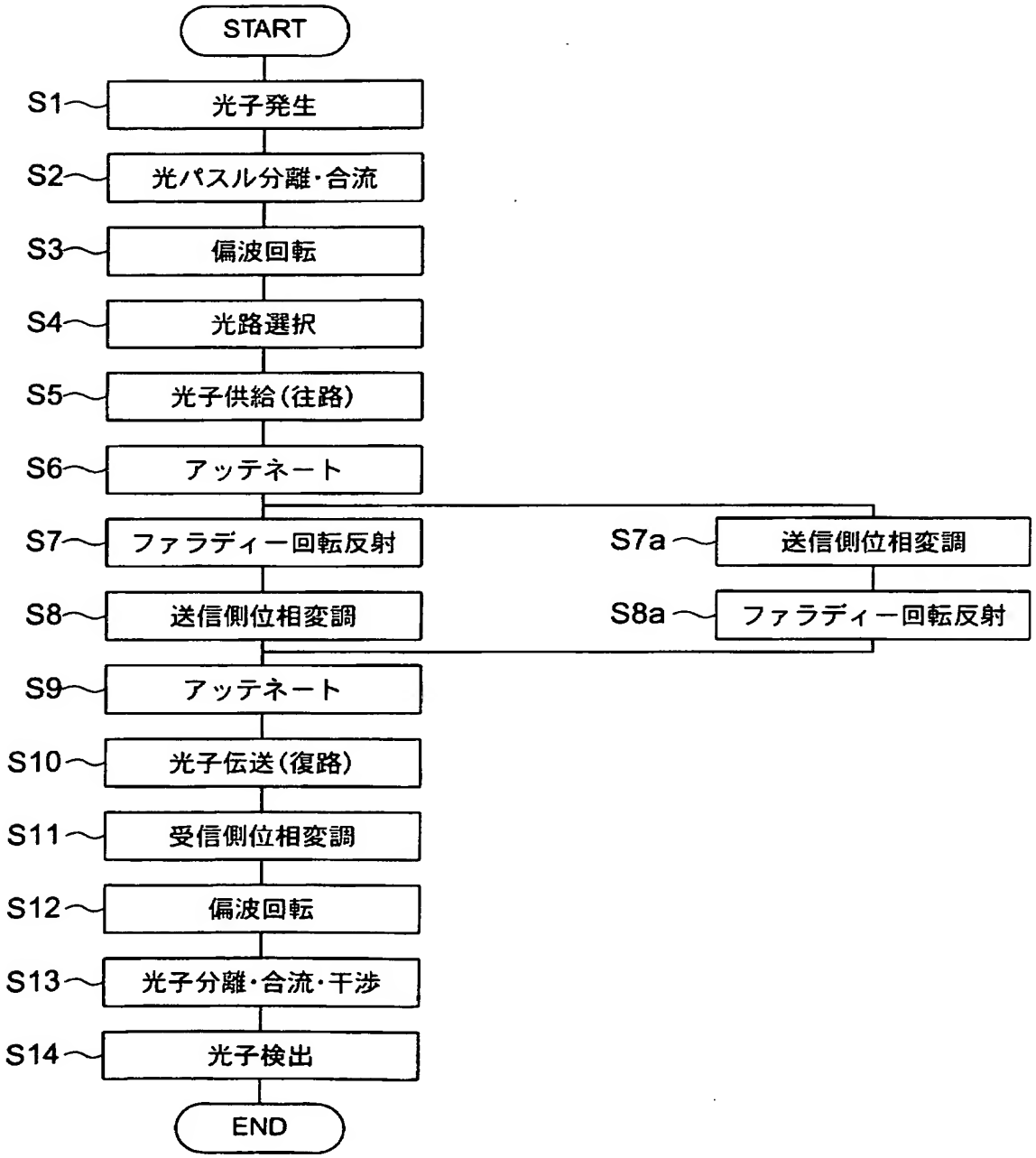

12
11
51
63
60
19
PolM
PM
18
61
62
4
13

図 7


START
S1
光子発生
S2
光パスル分離・合流
S3
偏波回転
S4
光路選択
S5
光子供給(往路)
S6
アッテネート
S7
ファラディー回転反射
S8
送信側位相変調
S7a
送信側位相変調
S8a
ファラディー回転反射
S9
アッテネート
S10
光子伝送(復路)
S11
受信側位相変調
S12
偏波回転
S13
光子分離・合流・干渉
S14
光子検出
END

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/007001

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁷ H04L9/12, H04B10/00, G02F1/01

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl⁷ H04L9/12, H04B10/00, G02F1/01

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JICST FILE(JOIS), WPI, INSPEC(DIALOG)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Tsuyoshi NISHIOKA, Hirokazu ISHIZUKA, Toshio HASEGAWA, Jun'ichi ABE: "Kanryugata Ryoshikagi Haifu", 2002 Nen Ango to Joho Security Symposium Yokoshu, 29 January, 2002 (29.01.02), Volume 1 of 2, pages 43 to 48	1-5
Y	Tsuyoshi NISHIOKA, Hirokazu ISHIZUKA, Toshio HASEGAWA and Jun'ichi ABE: "'Circular Type' Quantum Key Distribution", IEEE PHOTONICS TECHNOLOGY LETTERS, receive on 19 April, 2002 (19.04.02), Vol.14, No.4, pages 576 to 578	1-5

[x] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 03 August, 2004 (03.08.04)	Date of mailing of the international search report 24 August, 2004 (24.08.04)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/007001

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Toshio HASEGAWA, Tsuyoshi NISHIOKA, Hirokazu ISHIZUKA, Jun'ichi ABE, Mitsuru MATSUI, Shigeki TAKEUCHI: "Chokyori Ryoshi Ango Tsushin System Jikken", 2003 Nen Ango to Joho Security Symposium Yokoshu, 26 January, 2003 (26.01.03), Volume 2 of 2, pages 1125 to 1130	1-5
Y	Toshio HASEGAWA, Tsuyoshi NISHIOKA, Hirokazu ISHIZUKA, Jun'ichi ABE, Katsuhiro SHIMIZU, Mitsuru MATSUI and Shigeki TAKEUCHI: "An Experimental Realization of Quantum Cryptosystem", IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E85-A, No.1, 01 January, 2002 (01.01.02), pages 149 to 157	1-5

国際調査報告

国際出願番号 PCT／JP2004／007001

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl' H04L9/12, H04B10／00, G02F1／01

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int.Cl' H04L9/12, H04B10／00, G02F1／01

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2004年
日本国登録実用新案公報	1994－2004年
日本国実用新案登録公報	1996－2004年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

JICSTファイル（JOIS），WPI，INSPEC（DIALOG）

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	西岡毅，石塚裕一，長谷川俊夫，安部淳一：“環流型量子鍵配布” ２００２年暗号と情報セキュリティシンポジウム予稿集，２００２．０１．２９，Ｖｏｌｕｍｅ １ ｏｆ ２，ｐ．４３－４８	１－５
Y	Tsuyoshi Nishioka, Hirokazu Ishizuka, Toshio Hasegawa and Jun'ichi Abe: “ “Circular Type” Quantum Key Distribution” IEEE PHOTONICS TECHNOLOGY LETTERS, 2002.04.19受入, VOL14, NO.4, p.576-578	１－５

☒ C欄の続きにも文献が列挙されている。 ☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 03．08．2004	国際調査報告の発送日 24.8.2004
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員） 青木 重徳 5M 4229 電話番号 03－3581－1101 内線 3597

様式PCT／ISA／210（第2ページ）（2004年1月）

国際調査報告

国際出願番号 PCT／JP2004／007001

C（続き）. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	長谷川俊夫，西岡毅，石塚裕一，安部淳一，松井充，竹内繁樹：“長距離量子暗号通信システム実験” ２００３年暗号と情報セキュリティシンポジウム予稿集， ２００３．０１．２６，Ｖｏｌｕｍｅ ２ ｏｆ ２， ｐ．１１２５－１１３０	１－５
Y	Toshio HASEGAWA, Tsuyoshi NISHIOKA, Hirokazu ISHIZUKA, Jun'ichi ABE, Katsuhiro SHIMIZU, Mitsuru MATSUI and Shigeki TAKEUCHI: “An Experimental Realization of Quantum Cryptosystem”, IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, VOL. E85-A, NO. 1, 2002. 01. 01, p. 149-157	１－５